THE
NATIONAL LAW REVIEW

Cancer Care Group to Pay $750,000 to Settle HIPAA Breach, as KPMG Finds 81 Percent of Hospitals and Health Insurance Companies had a Breach in the Past Two Years

Article By
Joseph J. Lazzarotti
Jackson Lewis P.C.
Workplace Privacy Blog

- Communications, Media & Internet
- Consumer Protection
- Health Law & Managed Care

- All Federal

Tuesday, September 8, 2015

On September 2, the Office for Civil Rights (OCR) reported that it agreed to settle potential violations of the HIPAA privacy and security regulations with Cancer Care Group, Inc. The dollar amount of the settlement, $750,000, is significant, and the agreement to adopt a robust, multi-year corrective action plan under the watchful eye of the government is likely to be an unwanted strain on the business.

With 17 radiation oncologists, Cancer Care is by no means a mom and pop outfit, but it is also not a national provider. Small to mid-sized healthcare providers and their business associates need to take note. What started as a seemingly small theft issue – laptop bag stolen from an employee's car – has led to nearly a million dollars in settlement and other costs, and years of government monitoring of the practice's

privacy and security compliance.

Thinking your healthcare or related business will not experience a breach may not be a wise approach. According to a KPMG report, highlighted by ConsumerAffairs, in the past two years 81 percent of hospitals and health insurance companies have had a data breach. The question really is, however, will your business be able to stand up to an OCR compliance review that comes along with the OCR's investigation of the breach.

What happened: On August 29, 2012, OCR received notification from Cancer Care regarding a breach of unsecured electronic protected health information (ePHI) after a laptop bag was stolen from an employee's car. The bag contained the employee's computer and unencrypted backup media, which contained the names, addresses, dates of birth, Social Security numbers, insurance information and clinical information of approximately 55,000 current and former Cancer Care patients. A fairly typical scenario many businesses face, including health care providers, with the myriad of devices employees use every day in their jobs.

The OCR investigation: OCR claims Cancer Care was in "widespread non-compliance with the HIPAA Security Rule." According to OCR's press release, the provider "had not conducted an enterprise-wide risk analysis…did not have in place a written policy specific to the removal of hardware and electronic media containing ePHI into and out of its facilities, even though this was common practice within the organization." So you see, it was not so much the theft of the laptop, but the alleged lack of safeguards and compliance that could have (even if it in fact would not have) prevented the breach from happening, that drew the agency's ire.

OCR's Corrective Action Plan (CAP): You can read the CAP here. Under the CAP, you'll find that Cancer Care needs to get OCR's approval before it can proceed with key compliance steps. For example, it needs to provide its risk assessment to OCR within 90 days of the effective date of the settlement agreement, and await OCR's approval. A similar process applies for other components of the HIPAA security rules, including the development of a risk management plan and training program. Cancer Care must also provide an annual report to OCR for at least three years concerning updates or changes to its risk management plan, among a number of other things.

Take Away: No health care provider or other business wants to have a breach. But if it does, it will be less likely to face significant enforcement action by OCR if it has a compliance program in place – perform and document a risk assessment; address the risks of mobile devices; design and implement a quality training program. These are just a few of the steps a health care provider, health plan, business associate or other organization with HIPAA privacy and security obligations should be taking to mitigate these compliance risks.

Source URL: https://www.natlawreview.com/article/cancer-care-group-to-pay-750000-to-settle-hipaa-breach-kpmg-finds-81-percent